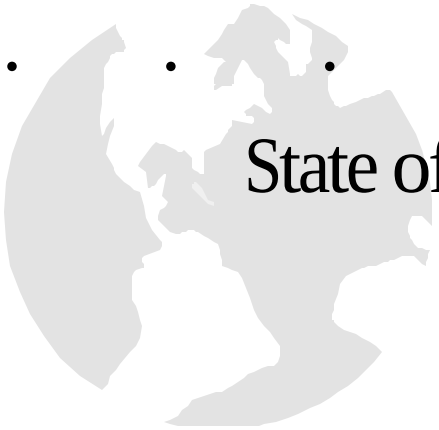
Protecting Personal Information in Electronic Records:

Managing Privacy and Access In E-Government



State of Georgia

Sponsored by:
Office of Secretary of State
Georgia Archives

Privacy and Access in Georgia E-Government
was made possible by a grant from the
National Historical Publications and Records Commission
2003-2004

Managing Privacy and Access in E-Government

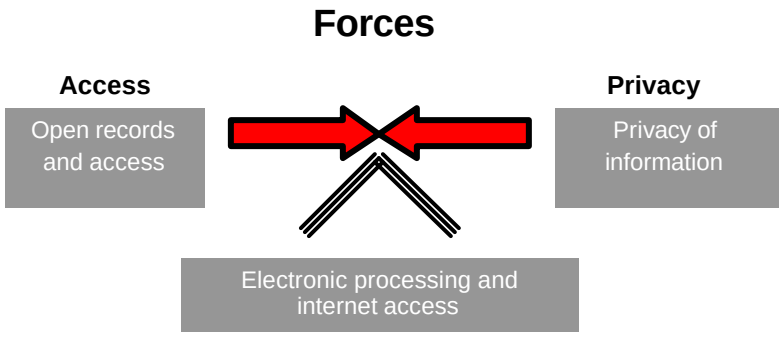
Executive Summary

Government has a virtual monopoly on the services it provides. In order to receive or participate in these services, **citizens must provide details on their life, activities, and personal characteristics to government agencies. Most citizens assume that this information is being held in confidence and protected from misuse and accidental release**. While government officials (citizens themselves) strive to protect this data, they must also provide reasonable access to government information in accordance with the Georgia Open Records Act (O.C.G.A. 50-18-90, et seq.) Paramount to the function of state government is this access by citizens and the media to its proceedings, operations, and records. Yet, as governments at all levels implement technology as the means to a better, more responsive and responsible government, the risks increase that confidential information may be released and cause harm and dissatisfaction with government as a whole.

In this regard, states have enacted open records statutes and the federal government, the Freedom of Information Act to ensure and protect access to government records. However, counterbalancing these efforts is the need to protect the privacy of citizens whose information the government collects and maintains from unwarranted invasion of personal privacy. Access to public records is not simply a yes-no proposition. There must be a balance between disclosure and non-disclosure that is guided by a combination of legislation, policy, and procedure. In Georgia government, this vital balancing act is performed by state employees who with little to no guidance must interpret the Open Records Act and determine if the information being requested should be released. As surveys and articles by the Atlanta Journal Constitution and others have shown, **compliance with the Open Records Act is inconsistent at best**.

Recent federal regulations have established requirements that will become standards for the protection of individually identifiable information in the health, education, and financial sectors. These regulations, which preempt state laws when necessary, establish a minimum level of compliance for protection of data. Poised between

these two equally important and opposing forces are the efforts of state government to improve efficiency and availability of services via electronic processing and the Internet.

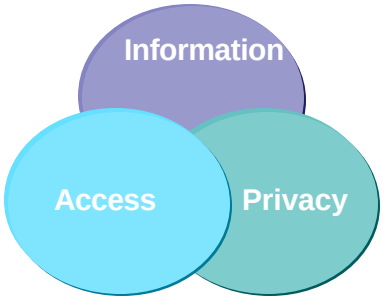


Caught in the middle of dwindling budgets and larger mandates, government has turned to technology to 'do more with less.' **The advent of electronic access to state records has now opened up volumes of data** that before were protected by the tedious steps required for collection and collation in the paper environment. What would have taken months previously, can now be accomplished remotely in minutes via search engines using desktop equipment. The Internet has also added to the potential impact by multiplying exponentially the opportunity for distribution of personal or private information.

Perhaps **one of the greatest tools at the disposal of government officials is the least used, records management**. Although a mandate of government, records management has been unevenly implemented with few agencies devoting a full time position to the task. Information is clogging the state's data center and agency networks and cluttering backup storage; information that could have been disposed of according to approved retention schedules. So long as this information remains in existence, it remains subject to an Open Records Act request, litigation, and investigation. **Few agencies have policies and procedures identifying confidential information** or guiding agency staff in answering requests for information.

These issues facing the state require the development of policies, and possibly legislation, that provide criteria for defining individually identifiable data, for determining secure classification levels, for defining organizational responsibility, and for enabling lifecycle management. Boundaries defining private information and delimiting access to it are required alongside those for physical security to assist the custodians of the records in properly adhering to open records requirements, while at the same time protecting against unauthorized disclosure of private information.

Because of their expertise and responsibility for state records, the Georgia Technology Authority and the Secretary of State – Georgia Archives should lead the development of these policies and procedures in a collaborative effort with other state and local agencies. **This collaborative effort should focus on the establishment of a life cycle management program for electronic records that includes the classification, maintenance and final disposition of electronic records through secure disposal or deposit into a Digital Archives.** The establishment of such a life cycle program is critical for the ongoing and legal maintenance of public records.



The following tasks are needed for the establishment of this program.

- Develop a statewide or enterprise-wide policy addressing the sharing, privacy and access to information.
- Require adoption and implementation of statewide policy.
- Develop model policies and procedures in support of agency policy and distribute them as best practices.
- Formalize a memorandum of agreement or other legal instrument for the sharing of information between agencies
- Establish certification of agency networks to establish compliance and integrity of information systems.
- Require the adoption of lifecycle management for all transactional data.
- Identify and categorize government created and maintained data.
- Preserve long-term and historical data.

Table of Contents

Background and Acknowledgements

In October 2002, the National Historical Publications and Records Commission (NHPRC) awarded the Office of Secretary of State, Georgia Archives (hereinafter referred to as the Georgia Archives) a grant to partner with Southern Polytechnic State University (SPSU) in order to present a series of workshops addressing privacy and access issues in e-government for Georgia's state and local governments and public universities. The grant award allowed the Georgia Archives to explore the issues of privacy in the digital age with a group of intensely interested public officials from around the state.

The "Privacy and Access Issues in Georgia E-Government Conference" was held on Wednesdays and Thursdays from July 16 through July 31. The presentations at the conference were paired each day so that a speaker discussed the national perspective on an issue and was followed by a second speaker discussing the issue from a statewide or agency perspective. A list of speakers and topics is included in the appendix. Each conference speaker was asked to address a different aspect of the issue of identity management and privacy:

- Requirements for policy to interpret law and establish procedure
- Compliance with laws, rules, and regulations
- Legal definitions and the application of law to digital identity
- Identification of elements within digital identity
- Managing identity through a portal application
- Lifecycle management of transactional data

Following the presentations, two days of working group meetings outlined the issues reflected in this white paper. The conference was held on the campus of Southern Polytechnic State University with a live audience of twenty-five, primarily state government officials. Utilizing the Georgia Statewide Academic and Medical System (GSAMS), the audience was broadened to include university, state, county, and municipal officials attending at five sites around the state. The conference focused on the collection, maintenance and use of individually identifiable data in the electronic applications of government.

The Office of Secretary of State, Georgia Archives gratefully acknowledges the support and participation of the following agencies and associations:

- Southern Polytechnic State University
- Georgia Records Association
- Society of Georgia Archivists
- Board of Regents, University System of Georgia
- Georgia Technology Authority

In addition, The Georgia Archives would like to acknowledge the work of members of the whitepaper author/editor group:

- Larry Bray, Georgia Technology Authority
- Jan McCord, Georgia State University
- Laurel Bowen, Georgia State University
- Anthony Mazza, Board of Pardons and Paroles
- Pamela Altman, University of Southern Georgia
- Dr. Richard Halstead-Nussloch, Southern Polytechnic State University
- Amelia Winstead, Georgia Archives
- Andrew Taylor, Georgia Archives
- David Carmicheal, Georgia Archives

Introduction

Citizens are required to provide certain information to government agencies in order to obtain services. Examples are applying for a driver's license, medical benefits, welfare support, payment of taxes, building permits as well as information provided in birth, death, and marriage certificates. Such data is used to establish and verify the identity of an individual, vendor or company in order to qualify that entity to receive government benefits, apply for a professional license, pay taxes, or establish residency and citizenship. Usually this information is retained by the government agency to confirm the transaction, issuance of license or services. In some instances, it is retained for statistical reports to justify future funding and resource allocation. The information is provided by the citizen in a semi-voluntary manner and carries the expectation of the citizen that it will be used solely for the purpose it was provided. Government holds a monopoly on the services it provides and collects tremendous amounts of detail on its customers. This information, if not properly managed, could be inadvertently released under the Georgia Open Records Act and used to establish alternate identities (for benefit purposes), destroy credit ratings, or defraud the government and the taxpayer out of funds and services.

"information is provided by the citizen in a semi-voluntary manner and carries the expectation . . . that it will be used solely for the purpose it was provided."

1. Scope and Objective

The organizational scope of the paper includes all entities of Georgia government mandated to conduct business on behalf of the citizenry and charged by the Georgia Open Records Act with providing reasonable access to the information government collects in the conduct of this business. This document addresses concerns for managing access to individually identifiable data maintained as part of electronic applications in government. Many of these same concerns and recommendations apply to information in other formats – i.e., paper or microfilm – however, for clarity and focus, only electronic media are addressed here.

This white paper, the product of the NHPRC grant, is intended to focus on the issues facing the state in terms of the potential risks involved, principles that need to be addressed, and ongoing recommendations for implementation. It is the desire of the authors that the paper serve as a vehicle for the formation of the policies and the next steps necessary for the protection of each citizen's information in an increasingly electronic environment. This paper provides a set of statements of intent that would form the basis for policies to safeguard privacy and proposes next step

recommendations for managing privacy through identification, classification, and records management.

2. State of Problem and Risks

Many details of an individual's life, activities, and personal characteristics can be found scattered throughout the files of government agencies. At the federal level, the privacy exemption in the Freedom of Information Act and the Privacy Act of 1974 prohibit the public disclosure of personal information contained in government files. At the state and local level, however, different types of records are maintained, and the laws and policies governing access and disclosure often lead to confusion, resulting in disparate results. As governments at all levels implement technology as the means to a better, more responsive and responsible government, the risks increase that confidential information may be released and cause harm and dissatisfaction with government as a whole.

The Problems

The problems facing Georgia in protecting its most valued asset, information, as we move towards better government for the citizens' benefit, can be discussed in terms of four needs:

- Privacy
- Access
- Accountability and Compliance
- Records Management

A. Privacy

There is a vast literature on the nature and scope of the right of privacy, but there is no consensus on the constitutional, legal, or general meaning of the concept of privacy. The U.S. Constitution guarantees individuals a right to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures; a right against self-incrimination; and a right to speak and assemble. These and other constitutional principles have been associated with privacy interests. The right of privacy has been analyzed as two separate interests: an interest in avoiding disclosure of personal matters and an interest in independence for personal decisions involving

marriage, procreation, contraception, family relationships, child rearing, and education.

As with other constitutional rights, there is no absolute right of privacy. Like the right of access, discussed below, privacy must always be balanced against other interests.

The Problem: "Like the right of access, . . , privacy must always be balanced against other interests."

Privacy in Georgia

Georgia's government agencies provide access to public records under provisions of the Open Records Act. This statute provides a process for responding to a request for information and provides some guidance on records and information that is not to be disclosed to the public. However, the statute does not define or protect a specific set of personal data across government. Having been developed and revised over a period of years, the current act, in many instances, addresses personal data of one population only – for example, law enforcement and judicial officials – while leaving the records of others open and available for access and possible misuse. The lack of clarity in the act is further compounded by the plethora of federal regulations and laws with which government must comply. The Health Insurance Portability and Accountability Act and the Graham-Leach-Bliley Act are two recent pieces of federal legislation that have resulted in privacy regulations.

B. Access

Public access to government records, activities, and proceedings serves several different and overlapping policy goals. Citizens need government to make political decisions about government programs, legislative and regulatory options, and candidates running for office. Knowledge about government is an important element in instilling confidence in the political system. Citizens need government information to assist in oversight of and accountability for government programs. Individuals need government information to know what services are provided by government. Government information is a valuable resource and commodity that can be used in many different ways to further economic growth. However, there are other interests and values that may be negatively affected by the public availability of government information, and most cases call for a balance of conflicting interests. Government records may need to be withheld from public disclosure to protect state and national defense interests, to foster law enforcement investigations, to support the deliberative processes of government, to protect the confidentiality of private business information, and to protect the privacy interests of individuals.

"Access to public records is not simply a yes-no proposition."

Access to public records is not simply a yes-no proposition. Mechanisms to ensure an appropriate balance between disclosure and non-disclosure must be implemented both through legislation, policy, and procedure.

Access in Georgia

In Georgia government, this vital balancing act is performed by state employees who with little to no guidance must interpret the Open Records Act and determine if the information being requested should be released. This results in inconsistent answers to requests for information from the public, between agencies, and often within an agency. Such uneven application of restrictions within the Open Records Act leads to frustration towards government on the part of the requester and the potential release of confidential information, resulting in a lack of trust that government will protect the citizen.

In addressing access to information via email or the Internet, the situation is compounded by lack of identity verification controls at both the state portal and agency application interface. Identity management is a process of verifying that "I am who I say I am." Lack of such controls means that there is the potential for confidential information to be viewed by unauthorized individuals. Or worse yet, that key electronic applications are not sufficiently protected from misuse or fraudulent data entry.

No single source of guidance on providing access to public records under the Open Records Act exists. Various agencies (Secretary of State and the Attorney General), organizations (First Amendment Association), and associations (Georgia Municipal Association and Association of County Commissioners, to name but two) provide training to state and local governments on how to manage access to public records. But even this training is a result of an interpretation of the Act with each group emphasizing different goals.

C. Accountability and Compliance

Today's government official and employee are confronted with the daily responsibility of providing access to government records while protecting the rights and privacy of the individual citizen and the government. The demand for access to government records through freedom of information legislation, coupled with the ease of access provided by the Internet and information technology have created a

crisis of resources and responsibility. Reduced budgets and staffing levels, and the absence of an established and supported policy for the protection of private information have resulted in an ongoing dilemma; provide information or face legal action for denying access; protect the privacy of an individual or release the information and destroy a life -- difficult choices faced every day in this state at the state, county, and municipal level.

Accountability and Compliance in Georgia

Each day, Georgia's government officials and employees conduct the public's business and, in the process, collect information about the public they serve. During the course of a day, these officials receive requests for information under the Open Records Act. Not only must these requests be answered within three working days, the official must also determine if the requested information may be released. But, does the Open Records Act apply to information? What about databases? Databases are amalgamations of information, are they records? In what media should I release the information – electronic or paper printout? What about email, is it a record? Do I still have the records? If so, where are they? These are just some of the questions that officials must answer before they can respond to the request. Oftentimes, lack of guidance and confusion result in the official responding with a negative – no, you may not have this information or that record. Better to deny access, rather than release confidential information. As surveys and articles by the Atlanta Journal Constitution and others have shown, compliance with the Open Records Act is inconsistent at best.

"As surveys and articles by the Atlanta Journal Constitution and others have shown, compliance with the Open Records Act is inconsistent at best."

D. Records Management

One of the greatest tools at the disposal of government officials is perhaps the least used, records management. Records management is the systematic control of all records from creation or receipt through processing, distribution, use, retrieval, and maintenance to their ultimate disposition. Basically, it is knowing what information you collect, how you use it, what is done with it, and where it is stored. Knowing your records provides direct value to the agency in assisting in the identification of confidential information; in streamlining data collection processes so that information is collected once and used many times; and, in lessening legal liability by ensuring the disposition of information after the legal and administrative need for the record has passed.

Records management practices and retention schedules require the identification of confidential information and the establishment of procedures protecting it. Strictly following the records management policies and schedules can be beneficial to both the citizen and the government. The citizen knows that his or her personal information will remain with government for the defined period of time and then be destroyed. At the same time, the agency benefits as well, in that it will not be in violation of its own records management practices and will not be forced to give out information that should not be accessed. Information held past the retention date remains subject to the Open Records Act.

Records Management in Georgia

Georgia's government agencies must manage their records for economy and efficiency under the provisions of the Georgia Records Act (O.C.G.A. 50-18-70 et seq). This same act mandates the Georgia Archives to operate a records management program to issue retention schedules and to provide guidance and assistance to state and local governments in the management of government records. In addition, further legislation establishes the Georgia Archives mandate to collect and preserve the history of the state.

A Possible Solution:

"Strictly following records management policies and schedules can be beneficial to both the citizen and the government."

Although a mandate of government, records management has been unevenly implemented with few agencies devoting a full time position to the task. Even then, the job of records management has been driven by the need to destroy vast amounts of paper rather than to systematically control and use information. As budgets have tightened and government has turned to technology to 'do more with less,' email, web portals, databases, and other electronic applications have been implemented with little to no regard for managing the information or for ensuring the creation of records. Information is clogging the state's data center and agency networks and cluttering backup storage. Much of this information could have been disposed of according to approved retention schedules. So long as this information remains in existence, it remains subject to an Open Records Act request, litigation, and investigation. Few agencies have policies and procedures identifying confidential information or guiding agency staff in answering requests for information. Even fewer provide training on these procedures so that all staff are aware and implement the procedures.

The Risks

What happens when Georgia government fails to protect confidential information? Already viewed with distrust, government will suffer further loss of public's trust. However, release of private information impacts the citizens of Georgia not as a body but as individuals through identity theft, financial loss, and possibly even personal injury. Terrorists could benefit by obtaining such information, making us all vulnerable to attack, vandalism, or other malicious activities. And, finally, there could be an economic impact on the state as government agencies are sued or made ineligible for federal monies as a result of non-compliance with federal and state law and regulation. Protecting confidential information is a matter of legislative direction, policy development, and implementation. Non-compliance in this area damages the individual, the public, the government, and ultimately, the state as a whole.

3. Statement of Intent on Part of State to Protect Data

The state of Georgia has a responsibility in the fulfillment of its duty to the citizens to safeguard the confidentiality and integrity of the electronic information that it collects and maintains. It is the intent of the state of Georgia to ensure the privacy of electronic information and to demonstrate that data protection is an objective of electronic government, not an obstacle to it. The statement of intent and related principles below provide a framework for the state to protect the privacy of electronic information of which it has custody.

Statement of Intent

The agencies and institutions of the state will protect the privacy of electronic data about its citizens and those who transact business with the state. To the extent permitted by federal and constitutional laws, the state of Georgia will not disseminate private information without the consent of the affected party.

A. Privacy

Principle

Privacy requires that individually identifiable information be protected against unauthorized access, dissemination, or alteration. Electronic information that is determined to be non-public and yet available via electronic means should be available for access, review, and annotation by the individual identified in the information.

Rationale

Essential to the issue of privacy is the prevention of unauthorized access and publication of individually identifiable information that would create harm to the respective party. Areas of disclosure of information related to health, finance, and education are protected by federal regulations and create a minimum threshold for the protection of related or otherwise state-controlled electronic information that should be protected against unauthorized access.

Closely connected to the protection of private data is the opportunity for the respective party to have access and the right of review. The affected party should be able to review the accuracy of the information and be provided a recourse or annotation, if the information maintained is deemed to warrant it due to misrepresentation, error, or other factors.

B. Access

Principle

Access to non-public information must be reviewed and authorized by the custodian of the information, with such access limited to a need to know basis and modified and terminated as changes in roles and responsibilities warrant.

The identity for electronic access of state information should be validated in relation to the nature and confidentiality of the data to be accessed.

Rationale

Access to electronic information is predicated upon the authorization of the person performing the access and the credentials required to ensure authenticity for the electronic session. The custodian for non-public data must be identified and authorization for access approved based on the classification of the data and the need to know of the requester.

Electronic credentials are required to ensure that the individual accessing the data has the proper authorization. These credentials should occur in greater levels on surety, commensurate with the likelihood of unauthorized access or the gravity of the impact of unauthorized disclosure.

C. Classification

Principle

Electronic information in the State's custody should be classified as to public or confidential to ensure proper access.

Non-public information should be further categorized based on the confidentiality and potential impact of unauthorized disclosure or alteration.

Rationale

Electronic information collected and maintained by the state should be classified by the state to correspond to its confidentiality and impact of unauthorized access or disclosure. Public information should be accessible by all state employees and citizens and is generally that which is non-individually identifiable or as required by law. Non-public information requires safeguards for its protection and should be further categorized based on the level of protection required by the impact of disclosure or legal requirement.

D. Open Records Requests and Privacy

Principle

Requests for electronic information from the State should be reviewed and private information redacted before release, with precautions taken to ensure that data provided cannot be aggregated so as to violate the privacy of the affected party.

Rationale

The state's Open Records Act requires access to state information, with a narrow list of exclusions; federal regulations may preempt state laws to protect information regarding such areas as health, education, and finance. Information that is non-public must not be released without consent of proper state entity. Such requests should be processed and approved by the privacy officer for the organization which has custody of the data requested.

Reasonable safeguards should be followed to ensure that data which is individually public can not be aggregated to create data that is classified as non-public. For example, demographics data related to health or finance that has been de-identified (personal information has been removed or scrambled) may be aggregated and when compared, used to reconstruct the identity of an individual and, therefore, gain access to otherwise private information.

E. System Certification

Principle

Electronic processing of information requires that resources of information technology such as applications, systems, etc., be reviewed for compliance with privacy and security practices to safeguard the access, dissemination, and alteration of electronic information before implementation in a production environment.

Rationale

Information technology resources provide the mechanisms for the access, processing, and retention of electronic information. New or updated processes need to be assessed to ensure that they comply with state policies and procedures related to privacy and security. The assessment should be completed before approval for implementation in a production environment.

F. Organization Responsibility

Principle

Each government agency is responsible for assigning functions related to the management and safeguarding of private electronic information in the agency's custody.

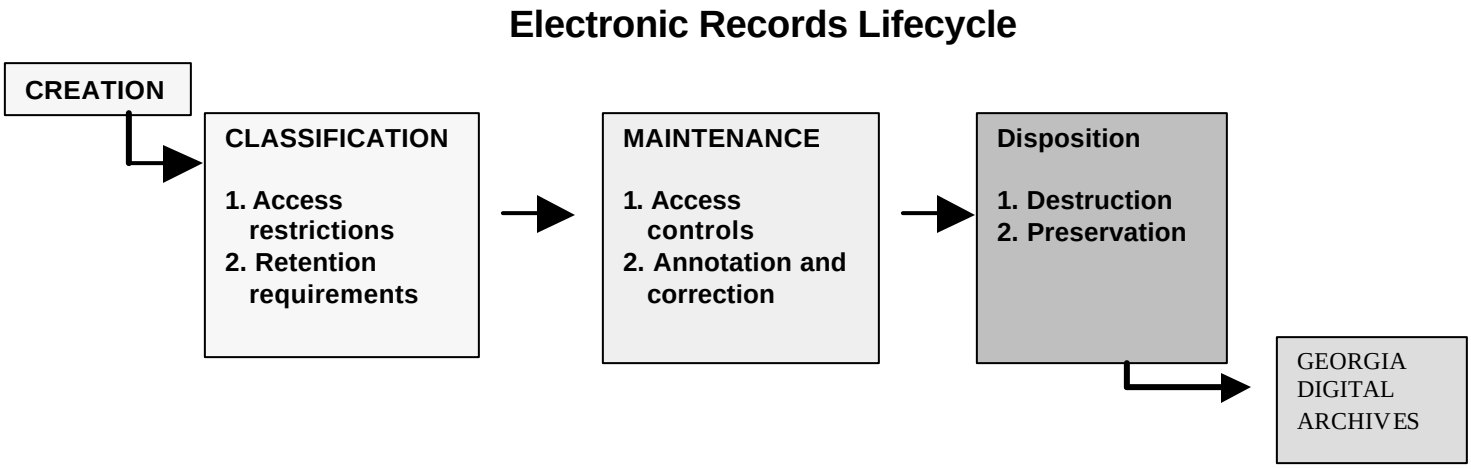
Rationale

The responsibility of ensuring the privacy of data within the state's custody should be assigned to a member of the organization. This assignment of responsibility must include such functions as necessary to ensure compliance with state and federal privacy regulations, assessment of privacy procedures, authorization and management of disclosure requests, proper reporting of unauthorized disclosures, etc.

4. Recommendations

The electronic data created and maintained by the State of Georgia needs to have a defined process that governs its life cycle. This life cycle must have the elements that provide for proper access via data classification and access controls, with prescribed custodial responsibilities assigned to the creator. These processes largely have been

developed and are practiced in the manual record environment, but corresponding rules are required to regulate the management of electronic records.



Traditionally, paper records were managed long after creation, once they were physically filed into agency filing systems and began to take up valuable office space. This management typically consisted of transferring the records offsite to a records center facility or warehouse dumping ground where they were forgotten. With electronic records, management must be included in system planning and implementation and must take place immediately upon creation as the agency classifies the information for further use. This classification is vital for the application of corresponding electronic controls to ensure appropriate access. The record management continues throughout the life cycle of the information, and if the information is of sustained value, should be continued by the Georgia Archives.

Working from the above process, you can see that several key components are currently absent from the state's legislative, programmatic and policy framework that prevent the implementation of a lifecycle management methodology. Each module of the process map above is discussed below. Within each are highlighted possible actions that will enable state government to achieve the reliable management of its electronic records.

A. Classification

Throughout the statutes of the state of Georgia there are references to information and records that are restricted from public access and exempted from the provisions of the Georgia Open Records Act (O.C.G.A. 50-18-70 et seq). The Open Records

Act itself places further restrictions on specific pieces of information. What results is a mass of laws that when combined with those federal regulations also applicable to state records, leaves local, state, and university officials confused yet scrambling to answer an information request within the three-day time frame of the Open Records Act. In such an environment, some restricted information may be missed (not redacted) and released to the requester.

Recommendations

1. Develop a statewide or enterprise-wide policy addressing the sharing, privacy and access to information.

2. Require adoption and implementation of statewide policy.

The development and use of electronic applications provides agency officials with an opportunity of identifying confidential data at its creation and providing protection for that data throughout its lifecycle through the application of security controls. However, to accomplish this, **agencies at all levels need a clear identification of what data is confidential and should be not be released to the public.**

The chart included in the appendices begins this work but further research is needed to include information restricted through such federal legislation as the Graham-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and the Family Educational Rights and Privacy Act. In addition, this information must be updated as laws and regulations change and presented in a usable format from a central location (possibly through a website linked to the state portal) enabling it to be referenced by government officials and citizens of the state of Georgia.

However, simply creating a clearinghouse for confidential data is not enough. Further **work is needed to provide government agencies with a legal definition of digital identity**. For all citizens, the identity for electronic access to government services must be defined and protected from misuse (e.g. name, Social Security Number, bank account number). Digital identity can be characterized or stated in terms of three elements.

> Digital identity is a set of pieces of information about a person that is needed to conduct a particular transaction; and, is not fixed but varies according to the requirements of the transaction.

In general, the more complex the transaction, the more information required to satisfy the identity requirements of the transaction. Not having a baseline set of data

elements identifying a person's identity for government results in an inconsistent milieu of definitions that agencies have determined based on their need at the time. **The state should define a minimum set of data elements that will provide a consistent basis for agencies to begin their policy and procedural development.**

B. Maintenance

The successful implementation of e-government applications in Georgia relies on the secure transmission of data between agencies, between the agency and the citizen, and between the citizen and the agency. Much of this data consists of individually identifiable data that if released or intercepted by a third party could result in loss or adverse impact to the citizen and the agency. Yet, there is currently no policy existing for the state of Georgia that clearly defines **the procedures and protocols that define or prescribe the handling of non-public data.** To ensure the successful implementation of existing and future e-government initiatives, the state develop the following infrastructure components:

- Statewide or enterprise-wide policy addressing the sharing of privacy and access to information must be developed and implemented. Such policy should begin with a statement of intent, such as the one included in this document, and move on to address the principles discussed in this document.
- Internal agency policy adopting and implementing procedures in support of statewide policy must be required to be developed by every agency of government.
- Model procedures in support of agency policy should be developed and shared through training and distribution as a best practice.
- Information sharing between agencies should be formalized through a memorandum of agreement or other legal instrument. This agreement would identify confidential information and define conditions of use and disclosure of this information (within the confines of the requirements of any state law) by the agencies.
- Prior to information sharing, agencies should be required to show network accreditation or system certification showing that their technology infrastructure is capable of protecting confidential information that may be

Recommendations

3. Develop model policies and procedures in support of agency policy.

4. Formalize a memorandum of agreement for sharing of information between agencies.

transmitted from another agency. These system certifications would also provide a level of confidence to the public that confidential information, once provided to an agency, could be protected by the agency.

C. Disposition

The transformation of the modern government office from a largely paper environment to an electronic environment presents a variety of problems and concerns for records management. Where once business was conducted via paper, today, email, web portals, databases and other electronic applications are the means by which government transacts business. Electronic information cannot be set aside and ignored in the same fashion as paper. Such information is only eye-readable through the interface of software and hardware. With each upgrade or change in software environment, we risk the loss of vital government information, much of it historical. Adding to the problem, by not managing the information through the use of retention schedules, we are increasing the volume of information clogging our networks, slowing retrieval times and increasing both the fiscal and legal liability of the agency.

Recommendations

5. Establish a certification of agency networks to establish compliance and integrity of information systems.

6. Require adoption of lifecycle management for all transactional data.

The **need for policy, procedure, and guidance guiding agencies in the disposition of electronic records** is critical, if we are to ensure the creation of legally-admissible transactional data; the preservation of the integrity of this transactional data for time periods sufficient to cover an audit or statutes of limitations; and, the authenticity of the party conducting the transaction as well as the authenticity of the transaction once conducted. Technology alone cannot address all these areas of concern. Agency policy and procedure must be developed and technology used in support of policy to ensure trustworthy, reliable record keeping in the electronic age. Key areas of policy and procedural development are:

- Lifecycle management of transactional data
- Identification and categorization of data
- Preservation of long-term and historical transactional data

In support of policy and procedural development should be the identification of codes of best practice at both the departmental and inter-departmental levels and the support of model projects that can be used as examples for the development of policy and technology in support of one another.

But who (or what agency) should lead the initiatives in e-records management? The Georgia Archives is charged by the Georgia Records Act (O.C.G.A. 50-18-70 et seq.) with developing policy and guidance in the management of government records, and with providing records management services to state and local governments. With limited staff and budget, it accomplishes this task through education and partnerships within government. With the charge already existing for records management coordination in government, it makes sense to strengthen this program and its mandate to include e-records management and policy development.

Recommendations

7. Identify and categorize government created and maintained data.

8. Preserve long-term and historical data.

D. Digital Archives

While most of the data currently being created and maintained by government should ultimately be destroyed, a small percentage of the data must be maintained as part of the state's historical record. The final challenge for the state of Georgia and the ending point of electronic records lifecycle is **the creation of a digital archives, specifically the Georgia Digital Archives.** This entity currently exists only in the minds of staff at the Georgia Archives and the Georgia Technology Authority. Together, we are planning for the preservation of the state's historical data.

5. Conclusion

Georgia state and local governments are improving the manner in which they view and manage information. Through compliance with the Open Records Act, government has recognized a need to know the content of the information they create and collect as well as the state and federal regulations and laws that govern the release of the information. The responsibility of providing access while also maintaining privacy has demonstrated an on-going need for records and information management programs. State and federal legislation require that structured records and information management programs be applied to electronic records. Record

keeping is no longer optional. It is a critical component in the administration of government.

The growth of these programs at the local level and the rebirth of them at the state agency level demonstrates a growing recognition that technology alone is not the solution. As public administrators and elected officials review their current record keeping practices an appreciation of the need to implement technology in compliance with business needs and regulations has become apparent.

Recognizing the need to protect privacy and addressing the recommendations and suggestions of this white paper is but one step in developing a statewide information management program. The importance of continued cooperation between the technology side of the house with the regulatory /business side is critical. State and local governments look to the Georgia Technology Authority and the Secretary of State to provide the leadership necessary to create the environment for the development and implementation of such a program. Such an environment will:

- Promote awareness and understanding among public administrators to communicate and share experiences and needs
- Determine policies and procedures that are needed
- Facilitate the implementation of policies and procedures on a corporate level, and
- Provide on-going support through resources and assessments.

The goal of creating and implementing a unified information management program is critical for government to take advantage of the benefits technology provides while retaining the confidence of the citizenry.

6. Appendices

Appendix A: List of Speakers and Topics

David Carmicheal is director of the Georgia Archives, a division of the Office of Secretary of State. Prior to joining the archives in the fall of 2000, Mr. Carmicheal was director of Knowledge Management, Records & Archives Office of Westchester County, New York. *(Welcome and Introduction)*

Richard Halstead-Nussloch, Ph.D., CPE, is an experienced computing and ergonomics professional who consults with industry when he is not teaching graduate and undergraduate courses in computer science, information technology, and software engineering at SPSU. He also serves as SPSU project manager to the Georgia Digital Academy. *(Facilitated sessions)*

Paul M.A. Baker, Ph.D., is the Associate Director of Policy Research for the Office of Technology Policy and Programs, Georgia Centers for Advanced Telecommunications Technology (GCATT), a division of the Georgia Research Alliance, located on the campus of the Georgia Institute of Technology. He also serves as Project Director for several research initiatives focused on technology and disabilities policy, as part of the Rehabilitation and Engineering Research Center (RERC) on Mobile Wireless Technologies for Persons with Disabilities, and the RERC on Workplace Accommodations. His current research focuses on the use and implementation of information and communication technologies in state and local governments, and development of tools for community assessment and policymaking with special emphasis on the tension between national security surveillance and privacy of individual's data, security in information systems, access to public data, and evaluation of the parameters influencing public sector information development. *(Policy Perspectives on Government Use of Citizen Data: Balancing the Need for Privacy)*

Richard Keck is a partner in the Telecommunications and Electronic Commerce Practice Group of Troutman Sanders LLP. Over the past several years, he has played an important role in the evolution of e-commerce and information law. He has been heavily involved in state and federal legislative reform, and he represents a variety of clients on matters such as electronic contracting and record keeping, privacy and data protection, information security, distributed computing, taxation of remote sales, removal of technology barriers, software and content licensing, and intellectual property strategy. *(Policy Perspectives on Government Use of Citizen Data: Balancing the Need for Privacy)*

Paula Arcioni is an information security manager for the New Jersey Office of Information Technology, Office of E-Government Services. She has extensive experience in the deployment and support of large-scale enterprise PKI, LDAP, and user provisioning services. In particular, she has well-honed expertise in identity management, digital signatures, encryption, and data confidentiality processes in B-to-G, G-to-G, and C-to-G environments. *(Let's Not Reinvent the Wheel: New Jersey as an Example)*

Odysseus Marcopolus was appointed Director of the Office of e-Government at the New Jersey Office of Information Technology in September 1999. He leads a team of forty-five technology professionals with one goal in mind: making New Jersey the *Online State.* New Jersey's e-Government initiative is aimed at redefining the way government and its constituents exchange information, goods and services. His responsibilities include the delivery of information and services through the award winning myNewJersey Portal along with the design and implementation of the technical infrastructure necessary to support the delivery of online services. His e-Government team includes of a blend of leading edge technologists and business experts who help craft the delivery of web-based government services.

Prior to joining the Office of Information Technology, he served as the Director of Information Technology at the New Jersey Division of Developmental Disabilities where he directed technology efforts on behalf of more than 8,000 employees at seventeen locations across the state. *(Let's Not Reinvent the Wheel: New Jersey as an Example)*

Kathryn Allen is a senior assistant attorney general specializing in the Open Records Act and issues relating to Open Government. She has served on the staff of the State Law Department since 1978. *(Laws, Rules, and Regulations Impacting Georgia E-Government)*

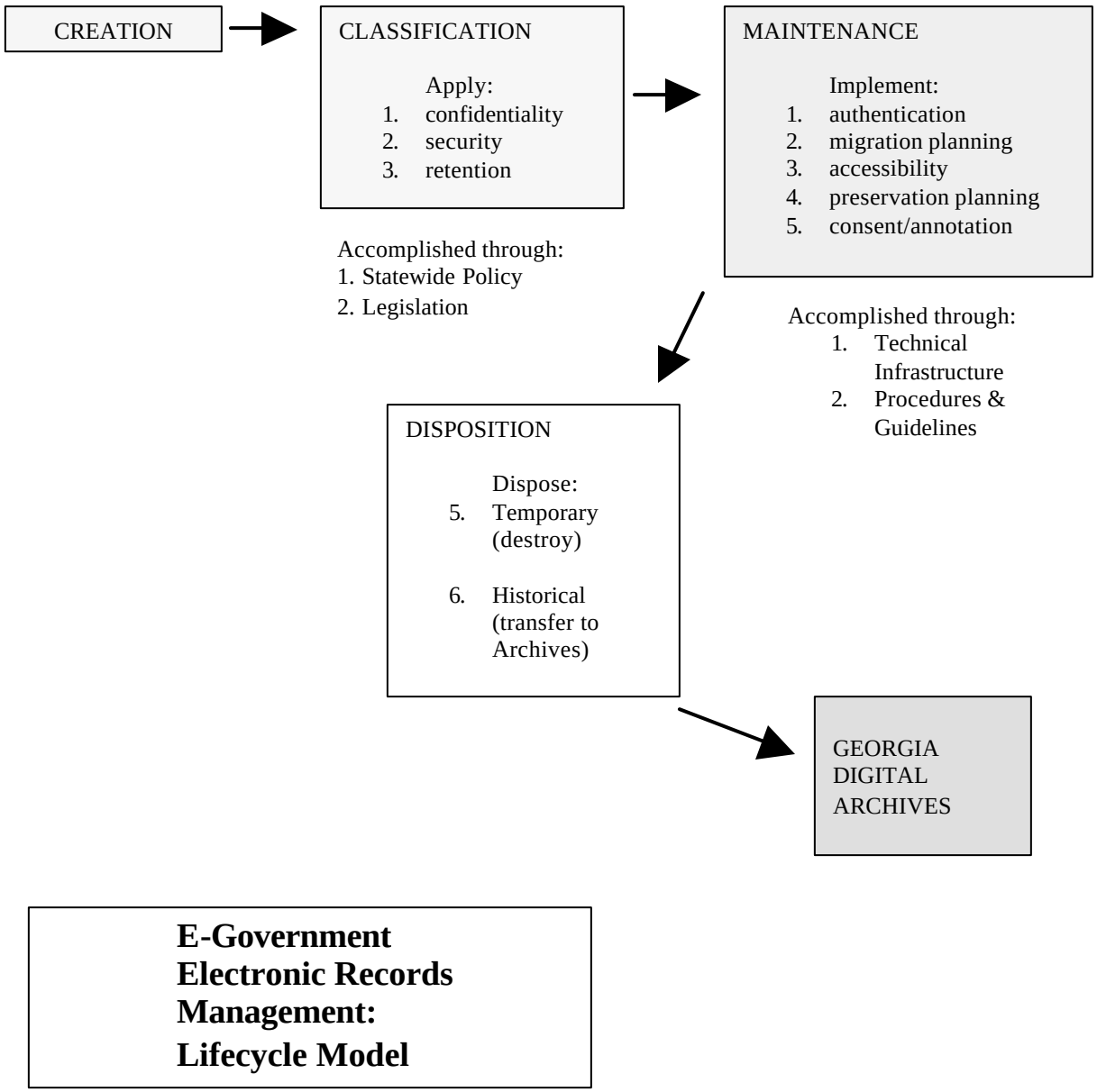
Emily Frye is the Director for Law and Economics at the Critical Infrastructure Protection Project of the National Center for Technology and Law, a think tank based within the George Mason University School of Law. Prior to joining George Mason University she served as president of her own consulting company specializing in the intersection of technology and law and also served as consulting attorney to iWitness, Motorola, Cohasset Associates, ABN AMRO, and Wilson Scientific. *(Digital Identity: A Discussion)*

John Graham is the Executive Director for Enterprise Application Systems at the Board of Regents of the University System of Georgia. He is in his 27th year in public education in Georgia which began with DeKalb County Board of Education. John held several jobs there before becoming the Payroll Manager at DeKalb

College, now Georgia Perimeter College, in 1986. He was hired to convert the payroll system of DeKalb College to that of the University System of Georgia when DeKalb College became the 34th unit of the University System. John held several jobs with DeKalb College before transferring to System Office in 1998. John has held several jobs in the System Office and was appointed Executive Director of Enterprise Application Systems about three years ago now. As Executive Director, John has major responsibility for all the administrative application systems of the University System including their student information systems, human resource systems, accounting systems, data warehouse and other administrative systems around their periphery. *(Protecting Personal Information)*

Charles M. Dollar is an internationally recognized expert on the life cycle management of electronic records, particularly electronic records archives. His experience includes: twenty years with the National Archives and Records Administration working with electronic records; archival educator at the University of British Columbia; consultant to governments and businesses in North America, Asia, Europe, and the Middle East; and, author of more than twenty publications on life cycle electronic records management issues. *(Planning for the Long-Term: When Digital Identity and E-Records must be Maintained)*

Appendix B: E-Government Electronic Records Management Lifecycle Model



Appendix C: Confidential Records According to Georgia Statute

Code Section	Agency	Description
2-7-68(a)	Agriculture, Dept. and Commissioner of	Confidentiality of trade secrets or commercial or financial information obtained from applicant for registration of pesticide.
2-8-29(b)	Agriculture, Dept. and Commissioner of	Confidentiality of information obtained pursuant to Code section 2-8-29.
2-13-5	Agriculture, Dept. and Commissioner of	Confidentiality of trade secrets concerning commercial feeds.
7-1-625(c)	Banking and Finance, Dept. of	Confidentiality of examinations of and reports pertaining to financial institutions.
7-1-702	Banking and Finance Dept. of	Confidentiality of Georgia Crime Information Center information concerning applicants for check cashier license.
7-1-1009(f)	Banking and Finance, Dept. of	Confidentiality of examinations and investigations of mortgage lenders and mortgage brokers.
10-1-207	Agriculture, Dept. and Commissioner of	Confidentiality of contents, formula, or trade secretes pertaining to ant/freeze.
10-1-760 et seq.	All agencies	Georgia Trade Secrets Act of 1990
12-8-29.2(a)	Natural Resources, Dept. of	Confidentiality of information relating to secret processes, devices, or methods of manufacture or production, or quantities and sources of recovered materials being privately processed, obtained by the Director of Environmental Protection Division of the Dept. of Natural Resources under the Georgia Comprehensive Solid Waste Management Act.
12-8-64	Natural Resources, Board of	Rulemaking authority to establish procedures to ensure protection of trade secrets and confidential information regarding hazardous waste general; or, hazardous waste transporters, and owners or operators of hazardous waste treatment, storage or disposal facilities.

Code Section	Agency	Description
12-9-19	Natural Resources, Dept. of	Confidentiality of information relating to secret processes, devices, or methods of manufacture or production obtained by the Environmental Protection Division of the Dept. of Natural Resources in the administration of the Georgia Air Quality Act.
12-13-21	Natural Resources, Dept. of	Confidentiality of records, reports, or information obtained pursuant to the Georgia Underground Storage Tank Act, upon a showing satisfactory to the Director of Environmental Protection Division of the Dept. of Natural Resources that such records, reports, or information, if divulged to the public, would divulge information entitled to protection under 18 USC 1905.
15-11-35.1	Corrections, Dept. of; Human Resources, Dept of; Juvenile Justice, Dept. of; and court ordering	Confidentiality of court-ordered HIV test results for a child adjudged to have committed a delinquent of; act constituting an AIDS transmitting crime HIV test.
15-12-67(a)	Superior Court Grand Jury members	Oath to keep secret the deliberations of the grand jury unless called upon to give evidence thereof in some court of law in the State of Georgia.
16-11-9	Attorney General	Confidentiality of records as may reflect on loyalty of any resident of the State of Georgia received and maintained under the Sedition and Subversive Activities Act of 1953.
19-7-5	Various governmental agencies	Confidentiality of reports of child abuse.
19-9-7	Georgia courts of competent jurisdiction and all government agencies	Court-ordered confidentiality of the address of a victim of family violence and her child.
24-9-21	Georgia Courts	Confidentiality of communications; between husband & wife or attorney & client; among grand jurors; as state secrets; between psychiatrist & patient; between patient and licensed clinical social worker, clinical nurse specialist in psychiatric/mental health, licensed marriage & family therapist, or licensed professional counselor during psychotherapeutic relationship; and, communications between these professionals regarding patient's otherwise privileged communications.

Code Section	Agency	Description
24-9-40	State-operated hospitals & health care facilities & physicians in government employ	Confidentiality of patient's medical information
25-4-8	Local & state law enforcement agencies	Confidentiality of conviction data regarding applicants for employment or certification as a firefighter.
30-5-7	Human Resources, Dept. of	Confidentiality of records pertaining to the abuse, neglect, or exploitation of disabled adults or elder persons in the custody of the Dept. of Human Resources.
31-5-5(a)	Human Resources, Dept. of; county boards	Confidentiality of documents, reports, & other information & data obtained by the Dept. of Human Resources and county boards of health relating to secret processes, formulas, and methods or obtained on a confidential basis.
31-10-25	Human Resources, Dept. of	Confidentiality of certain vital statistics.
31-21-3	State-operated hospitals & health care	Confidentiality of information regarding a deceased's infectious or communicable disease.
34-9-1(a)	Workers' Compensation, State Board of	Confidentiality of employers' names and employers' records.
35-3-30 et seq.	Georgia Crime Information Center	Confidentiality of and limited access to criminal records.
37-1-53	Human Resources, Dept. of	Confidentiality of documents, reports & other information relating to secret processes, formulas, and methods or where such matters were obtained or furnished on a confidential basis.
42-5-36	Corrections, Dept. of	Confidentiality of information supplied by inmates who cooperate in remedying abuses & wrongdoing in the penal system.
42-9-53(a)	Pardon & Paroles, State Board of	Confidentiality of information received by members of the State Board of Pardons & Paroles in the performance of their duties.
43-1-2(k)	State Examining Boards; Secretary of State	Confidentiality of certain records of the state examining boards.
43-34-37(a)13(c)	Medical Examiners, Composite Board of	Confidentiality of privileged information in results of mental or physical examinations required by the Composite Board of Medical Examiners.
43-39-16	Licensed psychologist in gov't employ	Confidentiality of communications between licensed psychologist and client.

Code Section	Agency	Description
45-20-15	State Merit System	Confidentiality of information received by State Merit System staff in counseling sessions with state employees.
46-5-168(e)	Public Service Commission	Confidentiality of trade secrets under the Telecommunications and Competition Development Act of 1995.
47-1-14	Public retirement systems created under Title 47 of OCGA	Confidentiality of certain specified records maintained by the retirement systems.
48-2-15	Revenue, Dept. of	Confidentiality of information secured by the Revenue Commissioner incident to the administration of any tax.
48-7-60	Revenue, Dept. of	Confidentiality of amount of income or particulars set forth or disclosed in any report or return.
48-7-170	Revenue, Dept. of	Confidentiality of information obtained by a claimant agency from the Dept. of Revenue in context of setoff debt collection.
49-5-40(b)	All agencies	Confidentiality of records concerning reports of child abuse and child controlled substance or marijuana abuse.
50-5A-11	Treasury and Fiscal Services, Office of	Confidentiality of certain records maintained by the Office of Treasury and Fiscal Services.
50-18-72(a)(1)	All agencies	Nondisclosure of records specifically required by federal government to be kept confidential.
50-18-72(a)(2)	All agencies	Nondisclosure of medical or veterinary records and similar files the disclosure of which would be an invasion of personal privacy.
50-18-72(a)(3)	Law Enforcement agencies	Nondisclosure of records compiled for law enforcement or prosecution purposes to the extent that production of such records would disclose the identity of a confidential source, disclose confidential investigative or prosecution material which would endanger the life or physical safety of any person or persons, or disclose the existence of a confidential surveillance or investigation.
50-18-72(a)(4)	Law Enforcement agencies	Nondisclosure of records of law enforcement prosecution, or regulatory agencies in any pending investigation or prosecution of criminal or unlawful activity, other than initial police arrest reports, accident reports, and incident reports.

Code Section	Agency	Description
50-18-72(a)(4.1)	All agencies	Nondisclosure of Georgia Uniform Motor Vehicle Accident reports, except upon submission of a written statement of need meeting the criteria established by this section and providing that a copy the report is made available to the individual's involved in the accident.
50-18-72(a)(5)	All agencies	Nondisclosure of records that consist of confidential evaluations submitted to or examinations prepared by a governmental agency and prepared in connection with the appointment or hiring of a public officer or employee.
50-18-72(a)(5)	All agencies	Nondisclosure of records consisting of material obtained in investigations related to the suspension, firing, or investigation of complaints against public officers or employees until ten days after the same has been presented to the agency or an officer for action or the investigation is otherwise concluded or terminated.
50-18-72(a)(6A)	All agencies	Nondisclosure of real estate appraisals, engineering or feasibility estimates, or other records made for or by the state or a local agency relative to the acquisition of real property until such time as the property has been acquired or the proposed transaction has been terminated or abandoned.
50-18-72(a)(6B)	All agencies	Nondisclosure of Dept. of Transportation engineers cost estimates and rejected or deferred bid proposals, except for the total amount of the bid, either received or prepared pursuant to Article 4 of Chapter 2 of Title 32 of the OCGA.
50-18-72(a)(7)	All agencies	Limited nondisclosure of portions of records which would identify persons applying for or under consideration for employment or appointment as executive head of an agency or of a unit of the University System of Georgia.
50-18-72(a)(8)	All agencies	Nondisclosure of records related to the provision of staff services to individual members of the General Assembly by the Legislative and Congressional Reapportionment Offices, the Senate Research Office, or the House Research Office.

Code Section	Agency	Description
50-18-72(a)(9)	All agencies	Nondisclosure of records that are of historical research value which are given or sold to public archival institutions, public libraries, or libraries of a unit of the Board of Regents of the University System of Georgia when the owner or donor of such records wishes to place restrictions on access to the records.
50-18-72(a)(10)	All agencies	Nondisclosure of records that contain information from the Dept. of Natural Resources inventory and register relating to the location and character of a historic property or properties if the Dept. through its Division of Historic Preservation determines that disclosure will create a substantial risk of harm, theft, or destruction of the property or area or place where the property or properties are located.
50-18-72(a)(11)	All agencies	Nondisclosure of records that contain site specific information regarding the occurrence of rare species of plants or animals or the location of sensitive natural habitats on public or private property if the Dept. of Natural Resources determines that disclosure will create a substantial risk of harm, theft, or destruction to the species or habitats or the area or place where they are located.
50-18-72(a)(11.1)	All agencies	Nondisclosure (or redaction) of an individual's social security number and insurance or medical information in personnel records.
50-18-72(a)(11.2)	All agencies	Nondisclosure of records revealing the names, home addresses, telephone numbers, security codes, or any other data developed, collected or received in connection with the installation, maintenance or operation of security systems, fire or burglar alarm systems provided that the incident reports will be accessible according to this section.
50-18-72(a)(11.3)(A-E)	All agencies	Nondisclosure of an individual's social security number, mother's birth name, credit card information, debit card information, bank account information and other personally identifiable data within the criteria established in this section.
50-18-72(a)(12)	All agencies	Nondisclosure of records containing information that would disclose or might lead to the disclosure of any component in the process used to execute or adopt an electronic signature.

Code Section	Agency	Description
50-18-72(a)(13)	All agencies	Personally identifiable data of law enforcement officers, judges, scientists employed by the Division of Forensic Sciences, correctional employees, and prosecutors or immediate family members or dependents thereof.
50-18-72(a)(13.1)	All agencies	Personally identifiable data of teachers or employees of a public school.
50-18-72(a)(14)	All agencies	Nondisclosure of personally identifiable information acquired for the purpose of establishing carpooling or ridesharing programs.
50-18-72(a)(15)	All agencies	Nondisclosure of security plans and vulnerability assessments, blueprints or other documents the disclosure of which could compromise security of public facilities or property.
50-18-72(a)(16)	All agencies	Nondisclosure of records from a 911 system that contain or would lead to the disclosure of personally identifiable data.
50-18-72(b)(1)	All agencies	Nondisclosure of data produced or collected by faculty or staff of state institutions during the conduct of research on commercial, scientific, technical, or scholarly issues.
50-18-72(b)(1)	All agencies	Nondisclosure of trade secrets obtained from a person or business entity.
50-18-72(b)(2)	All agencies	Nondisclosure of data collected or received by faculty, state, employees or students of an institution participating in the conduct of medical, scientific, technical, scholarly or artistic research.
50-18-72(b)(3)	All agencies	Nondisclosure of questions, scoring keys and other materials constituting a test that derives value from being unknown to the test taker prior to it being administered.
50-18-72(c)(2)	All agencies	Nondisclosure of personally identifiable data on individuals participating in research on commercial, scientific, technical, medical, scholarly or artistic issues.
50-18-72(d)	Probate courts	Nondisclosure of applications or other records submitted to the Probate Judge under provision of code section 16-11-129 relating to licenses to carry fire arms.

Code Section	Agency	Description
50-18-72(e)(1)	Legal counsels	Recognition of attorney-client privilege of nondisclosure.
50-18-72(e)(2)	Legal counsels	Confidentiality of attorney work product.
50-18-72(e)(3)	All agencies	Reaffirming confidentiality of certain tax matters.
50-18-72(f)(2)	All agencies	Exclusion of computer programs & computer software from terms of act.
50-27-25(a)	Georgia Lottery Corporation	Confidentiality of information relating to the operation of the Georgia Lottery.

Confidentiality Table: Jan. 2004